

# **FIPS 201 Evaluation Program - Electronic Personalization Test Procedure**

Version 2.0.0  
August 7, 2006



## Document History

<b>Status</b>	<b>Version</b>	<b>Date</b>	<b>Comment</b>	<b>Audience</b>
Draft	0.0.1	04/28/06	Document creation.	Limited
Draft	0.0.2	05/11/06	Document update.	Limited
Draft	0.1.0	05/11/06	Submitted to GSA for approval.	GSA
Draft	0.1.1	05/11/06	Changes made per GSA comment.	Limited
Approved	1.0.0	05/11/06	Approved by GSA.	Public
Revision	1.0.1	06/29/06	Updated based on feedback from GSA.	Limited
Revision	1.1.0	06/29/06	Submitted to GSA for approval.	GSA
Revision	1.1.1	07/31/06	Updated based on feedback from GSA.	Limited
Revision	1.1.2	08/04/06	Updated based on internal review	Limited
Revision	1.2.0	08/04/06	Submitted to GSA for approval	GSA.
Approved	2.0.0	08/07/06	Approved by GSA.	Public

## Table of Contents

<b>1</b>	<b>Overview .....</b>	<b>1</b>
1.1	Identification .....	1
<b>2</b>	<b>Testing Process .....</b>	<b>2</b>
<b>3</b>	<b>Test Procedure for Electronic Personalization .....</b>	<b>3</b>
3.1	Requirements .....	3
3.2	Test Components .....	22
3.2.1	Baseline Configuration .....	22
3.2.2	Components Details .....	22
3.3	Test Cases .....	23
3.3.1	Test Case EP-TP.1 .....	23
3.3.1.1	<i>Purpose</i> .....	24
3.3.1.2	<i>Test Setup</i> .....	24
3.3.1.3	<i>Test Process</i> .....	25
<b>4</b>	<b>Electronic Personalization Test Application Screens .....</b>	<b>26</b>
4.1	Testing Screen.....	26
4.2	Test Report Screen.....	26

## List of Tables

Table 1 - Applicable Requirements .....	22
Table 2 - Test Procedure: Components.....	23

# 1 Overview

Homeland Security Presidential Directive-12 (HSPD-12) - "*Policy for a Common Identification Standard for Federal Employees and Contractors*" directed the promulgation of a new Federal standard for a secure and reliable form of identification issued by all Federal Agencies to their employees and contractors.

In addition to derived test requirements developed to test conformance to the NIST standard, GSA has established interoperability and performance metrics to further determine product suitability. Vendors whose products and services are deemed to be conformant with NIST standards and the GSA interoperability and performance criteria will be eligible to sell their products and services to the Federal Government.

## 1.1 Identification

This document provides the detailed test procedure that needs to be executed by the Lab in order to evaluate the Electronic Personalization Product or Service against the subset of applicable requirements that need to be electronically tested for this category.

## 2 Testing Process

As previously mentioned, this document prescribes detailed test steps that need to be executed in order to test the requirements applicable for this category. Please note that conformance to the tests specified in this document will not result in the Product or Service being compliant to the applicable requirements of FIPS 201. The Product or Service must undergo an evaluation using all the evaluation criteria listed for that category prior to being deemed as compliant. Only products and services that have successfully completed the entire Approval Process will be designated as conformant to the Standard. To this effect, this document only provides details for the evaluation using the Lab Test Data Report approval mechanism.

A Lab Engineer follows the steps outlined below in order to test those requirements that have been identified to be electronically tested. The end result is a compilation of the observed behavior of the submitted PIV Card in the Lab Test Data Report.

Section 3 provides the test procedures that need to be executed for evaluating the Product or Service as conformant to the requirements of FIPS 201.

### 3 Test Procedure for Electronic Personalization

#### 3.1 Requirements

The following table provides a reference to the requirements that need to be electronically tested within the Lab as outlined in the Approval Procedures document for the Product and Service. The test cases that are used to check compliance to the requirements are cross-referenced in the table below.

Identifier #	Requirement Description	Source	Test Case #
EP.1	To activate the card for personalization or update, Application Administrator shall be authenticated to the PIV Card using a challenge response protocol which requires the use of cryptographic keys stored on the card. The authentication procedure shall be in accordance with SP 800-73-1.	FIPS 201, Section 4.1.6.2	EP-TP.1
EP.8	The personalized card shall be tested to the SP 800-85B test tool for data format compliance.	Derived	EP-TP.2
EP.9	Part 3 conformant cards shall return all the Tag-Length-Value (TLV) elements of a container in the physical order listed for that container in this data model.	SP 800-73-1-1, Appendix A	EP-TP.2
EP.10 <sup>1</sup>	The CCC shall identify the registered data model number 0x10.	SP 800-73-1-1, Appendix A	EP-TP.2
EP.11	The CHUID on a PIV card shall meet the following requirements: <ul style="list-style-type: none"> <li>The Federal Agency Smart Credential Number (FASC-N) shall be consistent with the Technical Implementation Guidance Smart Card Enabled Physical Access Control System (TIG SCEPACS) Option for “System Code    Credential Number” to establish a</li> </ul>	SP 800-73-1-1, Section 1.8.3	EP-TP.2

<sup>1</sup> This requirement number reflects the Electronic Personalization (Product) approval procedure. For testing of service-based Electronic Personalization, the applicable requirements for lab testing begin at EP.11 in the Electronic Personalization (Service) approval procedure.

	<p>credential number space of 9,999,999,999 credentials.</p> <ul style="list-style-type: none"> <li>The Global Unique Identifier (GUID) field must be present, and may include either an issuer assigned IPv6 address or be coded as all zeros. The GUID is included to enable future migration away from the FASC-N into a robust numbering scheme for all issued credentials.</li> <li>The Expiration Date is tagged 0x35 and value is within the next five years. This field shall be 8 bytes in length and shall be encoded as YYYYMMDD.</li> </ul>		
EP.12	The fingerprint buffer specifies the primary and secondary fingerprints within Tag value 0xBC.	SP 800-73-1-1, Appendix A	EP-TP.2
EP.13	The secondary fingerprint contained in the fingerprint buffer shall be preceded by the Tag value 0xBD.	SP 800-73-1-1, Appendix A	EP-TP.2
EP.14	The fingerprint template length shall not exceed 4,000 bytes.	SP 800-73-1-1, Appendix A	EP-TP.2
EP.15	The facial image is preceded with tag value 0xBC	SP 800-73-1-1, Appendix A	EP-TP.2
EP.16	The facial image length shall not exceed 12,710 bytes	SP 800-73-1-1, Appendix A	EP-TP.2
EP.17	The message digest produced as a result of a hash function on the contents of a data object buffer shall be identical to that data object's message digest contained in the security object.	Derived	EP-TP.2
EP.18	The CBEFF structure must comply with SP80076 Table 7, "Simple CBEFF Structure."	SP 800-76, Section 6	EP-TP.2
EP.19	The CBEFF header must comply with SP80076 Table 8, "Patron Format PIV	SP 800-76, Section 6	EP-TP.2

	Specification.”		
EP.20	The Patron Header Version of the CBEFF Patron Format shall be 0x03.	SP 800-76, Section 6	EP-TP.2
EP.21	The biometric data block is digitally signed but not encrypted, and this shall be reflected by setting the value of the Signature Block Header (SBH) security options field to b00001101.	SP 800-76, Section 6	EP-TP.2
EP.22	For fingerprint and facial records, the Biometric Data Block (BDB) Format Owner shall be 0x001B denoting M1, the INCITS Technical Committee on Biometrics.	SP 800-76, Section 6	EP-TP.2
EP.23	For the mandatory fingerprint template on the PIV card, the BDB Format Type value shall be 0x0201. For the optional facial image on the PIV card, the BDB Format Type value shall be 0x0501.	SP 800-76, Section 6	EP-TP.2
EP.24	The Creation Date in the PIV Patron Format (see Row 7 in Table 8 of SP80076) shall be the date of acquisition of the parent sample, encoded in eight bytes using a binary representation of "YYYYMMDDhhmmssZ". Each pair of characters (for example, "DD") is coded in 8 bits as an unsigned integer where the last byte is the binary representation of the ASCII character Z which is included to indicate that the time is represented in Coordinated Universal Time (UTC). The field "hh" shall code a 24 hour clock value.	SP 800-76, Section 6	EP-TP.2
EP.25	The Validity Period in the PIV Patron Format (Row 8 in Table 8 of SP80076) contains two dates.	SP 800-76, Section 6	EP-TP.2
EP.26	Biometric Type field within the PIV Patron Format shall be 0x000008 for fingerprint template and shall be 0x000002 for facial images. The	SP 800-76, Section 6	EP-TP.2



	value for other biometric modalities shall be that given in CBEFF, 5.2.1.5. For modalities not listed there the value shall be 0x00.		
EP.27	For the mandatory fingerprint template on the PIV card, the CBEFF Biometric Data Type encoding value shall be b100xxxxx, which corresponds to biometric data that has been processed. For the optional facial image on the PIV card, the CBEFF Biometric Data Type encoding value shall be b001xxxxx.	SP 800-76, Section 6	EP-TP.2
EP.28	For all biometric data whether stored on a PIV card or otherwise retained by agencies the quality value shall be a signed integer between -2 and 100 per the text of INCITS 358. A value of -2 shall denote that assignment was not supported by the implementation; a value of -1 shall indicate that an attempt to compute a quality value failed. Values from 0 to 100 shall indicate an increased expectation that the sample will ultimately lead to a successful match. The zero value required by FACESTD shall be coded in this CBEFF field as -2.	SP 800-76, Section 6	EP-TP.2
EP.29	The Creator field in the PIV Patron Format contains 18 bytes of which the first K <= 17 bytes shall be ASCII characters, and the first of the remaining 18-K shall be a null terminator (zero).	SP 800-76, Section 6	EP-TP.2
EP.30	The Data Type Encoding field in the PIV Patron Format shall contain the 25 bytes of the FASC-N component of the CHUID identifier.	SP 800-76, Section 6	EP-TP.2
EP.31	The “Reserved for future use” field in the PIV Patron Format shall contain 0x00000000.	SP 800-76, Section 6	EP-TP.2
EP.32	Both finger’s template records shall	FIPS 201-1,	EP-TP.2

	be wrapped in a single CBEFF structure prior to storage on the PIV card.	Section 4.4.2	
EP.33	The fingerprint templates stored on the card are compliant to the MINUSTD profile specified in SP80076, Table 3.	SP 800-76, Section 3.3.2	EP-TP.2
EP.34	The Format Identifier of the General Header Record shall be 0x464D5200.	SP 800-76, Section 3.3.2	EP-TP.2
EP.35	The Version Number of the General Header Record shall be 0x20323000.	SP 800-76, Section 3.3.2	EP-TP.2
EP.36	The length of the entire CBEFF wrapped record shall fit within the container size limits specified in SP80073.	Derived	EP-TP.2
EP.37	Both of the two fields ("Owner" and "Type") of the CBEFF Product Identifier shall be non-zero.	SP 800-76, Section 3.3.2	EP-TP.2
EP.38	The two most significant bytes of each of the two fields ("Owner" and "Type") of the CBEFF Product Identifier shall identify the vendor, and the two least significant bytes shall identify the version number of that supplier's minutiae detection algorithm.	SP 800-76, Section 3.3.2	EP-TP.2
EP.39	The Capture Equipment Compliance of the General Record Header shall be 1000b.	SP 800-76, Section 3.3.2	EP-TP.2
EP.40	The Capture Equipment ID of the General Record Header is greater than zero.	SP 800-76, Section 3.3.2	EP-TP.2
EP.41	The width on Size of Scanned Image in X Direction shall be the larger of the widths of the two input images. Similarly, the height on Size of Scanned Image in Y Direction shall be the larger of the heights of the two input images.	SP 800-76, Section 3.3.2	EP-TP.2

EP.42	The Number of Views of the General Header Record shall be 2.	SP 800-76, Section 3.3.2	EP-TP.2
EP.43	The Reserved Byte of the General Header Record shall be 0.	SP 800-76, Section 3.3.2	EP-TP.2
EP.44	The View Number of the Single Finger View Record shall be 0.	SP 800-76, Section 3.3.2	EP-TP.2
EP.45	The Impression Type of the Single Finger View Record shall be either 0 or 2.	SP 800-76, Section 3.3.2	EP-TP.2
EP.46	The quality value of captured fingerprint images shall be computed using NFIQ and reported as $Q = 20(6 - \text{NFIQ})$ .	SP 800-76, Section 3.3.2	EP-TP.2
EP.47	The Number of Minutiae of Single Finger View Record is between 0 and 128.	SP 800-76, Section 3.3.2	EP-TP.2
EP.48	Fingerprint templates shall be limited to minutiae of types "ridge ending" and "ridge bifurcation" unless it is not possible to reliably distinguish between a ridge ending and a bifurcation, in which case the category of "other" shall be assigned and encoded as 00b.	SP 800-76, Section 3.3.2	EP-TP.2
EP.49	All coordinates and angles for fingerprint minutiae shall be recorded with respect to the original finger image. They shall not be recorded with respect to any image processing sub-image(s) created during the template creation process.	SP 800-76, Section 3.3.2	EP-TP.2
EP.50	The mandatory value for Extended Data Block Length for MINUSTD template shall be zero.	SP 800-76, Section 3.3.2	EP-TP.2
EP.51	All facial images must conform with the requirements in SP80076 Table 6, "INCITS 385 Profile for PIV Facial Images."	SP 800-76, Section 5.2	EP-TP.2

EP.52	If facial imagery is stored on the PIV card, the length of the entire record shall fit within the container size limits specified in SP80073.	Derived	EP-TP.2
EP.53	PIV facial images shall conform to the Full Frontal Image Type defined in Section 8 of FACESTD.	SP 800-76, Section 5.2	EP-TP.2
EP.54	Facial image data shall be formatted in one of the two compression formats enumerated in Section 6.2 of FACESTD. Both whole-image and single-region-of-interest (ROI) compression are permitted.	SP 800-76, Section 5.2	EP-TP.2
EP.55	Facial images shall be compressed using a compression ratio no higher than 15:1. However, when facial images are stored on PIV cards, JPEG 2000 shall be used with ROI compression in which the innermost region shall be centered on the face and compressed at no more than 24:1.	SP 800-76, Section 5.2	EP-TP.2
EP.56	The CHUID buffer shall contain an Asymmetric digital signature of the CHUID object, which has been encoded as a Cryptographic Message Syntax external digital signature as defined in RFC 3852.	FIPS 201-1, Section 4.2.2	EP-TP.2
EP.57	The digital signature is implemented as a SignedData Type.	FIPS 201-1, Section 4.2.2	EP-TP.2
EP.58	The value of the version field of the SignedData content type shall be v3.	FIPS 201-1, Section 4.2.2	EP-TP.2
EP.59	The digestAlgorithms field of the SignedData content type shall be in accordance with Table 3-3 of SP80078.	FIPS 201-1, Section 4.2.2	EP-TP.2
EP.60	The eContentType of the encapContentInfo shall be id-PIV-CHUIDSecurityObject (OID = 2.16.840.1.101.3.6.1).	FIPS 201-1, Section 4.2.2	EP-TP.2

EP.61	The encapContentInfo of the SignedData content type shall omit the eContent field.	FIPS 201-1, Section 4.2.2	EP-TP.2
EP.62	The certificates field shall include only a single X.509 certificate which is used to verify the signature in the SignerInfo field.	FIPS 201-1, Section 4.2.2	EP-TP.2
EP.63	The crls field from the SignedData content type shall be omitted.	FIPS 201-1, Section 4.2.2	EP-TP.2
EP.64	The SignerInfos in the SignedData content type shall contain only a single SignerInfo type.	FIPS 201-1, Section 4.2.2	EP-TP.2
EP.65	The SignerInfo type shall use the issuerAndSerialNumber choice for the sid and this shall correspond to the issuer and serialNumber fields found in the X.509 certificate for the entity that signed the CHUID.	FIPS 201-1, Section 4.2.2	EP-TP.2
EP.66	The SignerInfo type shall specify a digestAlgorithm in accordance with Table 3-3 of SP 800-78.	SP 800-78, Section 3.2.1	EP-TP.2
EP.67	The signedAttrs of the SignerInfo shall include the MessageDigest (OID = 1.2.840.113549.1.9.4) attribute containing the hash computed over the concatenated content of the CHUID, excluding the asymmetric signature field.	FIPS 201-1, Section 4.2.2	EP-TP.2
EP.68	The signedAttrs of the SignerInfo shall include the pivSigner-DN (OID = 2.16.840.1.101.3.6.5) attribute containing the subject name that appears in the X.509 certificate for the entity that signed the CHUID.	FIPS 201-1, Section 4.2.2	EP-TP.2
EP.69	The signatureAlgorithm field specified in the SignerInfo field shall be in accordance with Table 3-4 of SP 800-78 and based on the PIV card expiration date in accordance with	SP 800-78, Section 3.2.1	EP-TP.2

	Table 3-3 of SP 800-78.		
EP.70	The SignedData content type shall include the digital signature.	FIPS 201-1, Section 4.2.2	EP-TP.2
EP.71	The digital signature certificate used to sign the CHUID shall in the extKeyUsage assert id-PIV-content-signing (OID = 2.16.840.1.101.3.6.7).	FIPS 201-1, Section 4.2.2	EP-TP.2
EP.72	The size of the public key for digital signature certificate used to sign the CHUID shall be determined by the expiration of the Card in accordance with Table 3-3 of SP 800-78.	SP 800-78, Section 3.2.1	EP-TP.2
EP.73	The CBEFF_SIGNATURE_BLOCK shall be encoded as a Cryptographic Message Syntax external digital signature as defined in RFC 3852.	FIPS 201-1, Section 4.4.2	EP-TP.2
EP.74	The digital signature is implemented as a SignedData Type.	FIPS 201-1, Section 4.4.2	EP-TP.2
EP.75	The value of the version field of the SignedData content type shall be v1 or v3 based on whether the certificates field is omitted or not.	FIPS 201-1, Section 4.4.2	EP-TP.2
EP.76	The digestAlgorithms field of the SignedData content type shall be in accordance with Table 3-3 of SP 800-78.	FIPS 201-1, Section 4.4.2	EP-TP.2
EP.77	The eContentType of the encapContentInfo shall be id-PIV-biometricObject (OID = 2.16.840.1.101.3.6.2).	FIPS 201-1, Section 4.4.2	EP-TP.2
EP.78	The encapContentInfo of the SignedData content type shall omit the eContent field.	FIPS 201-1, Section 4.4.2	EP-TP.2
EP.79	If the signature on the fingerprint biometric was generated with a different key as the signature on the CHUID, the certificates field shall include only a single certificate in the	FIPS 201-1, Section 4.4.2	EP-TP.2

	SignerInfo field which can be used to verify the signature; else the certificates field shall be omitted.		
EP.80	The crls field from the SignedData content type shall be omitted.	FIPS 201-1, Section 4.4.2	EP-TP.2
EP.81	The signerInfos in the SignedData content type shall contain only a single SignerInfo type.	FIPS 201-1, Section 4.4.2	EP-TP.2
EP.82	The SignerInfo type shall use the issuerAndSerialNumber choice for the sid and this shall correspond to the issuer and serialNumber fields found in the X.509 certificate for the entity that signed the biometric data.	FIPS 201-1, Section 4.4.2	EP-TP.2
EP.83	The SignerInfo type shall specify a digestAlgorithm in accordance with Table 3-3 of SP 800-78.	SP 800-78, Section 3.2.1	EP-TP.2
EP.84	The signedAttrs of the SignerInfo shall include the MessageDigest (OID = 1.2.840.113549.1.9.4) attribute containing the hash of the concatenated CBEFF_HEADER and the STD_BIOMETRIC_RECORD.	FIPS 201-1, Section 4.4.2	EP-TP.2
EP.85	The signedAttrs of the SignerInfo shall include the pivSigner-DN (OID = 2.16.840.1.101.3.6.5) attribute containing the subject name that appears in the X.509 certificate for the entity that signed the fingerprint biometric data.	FIPS 201-1, Section 4.4.2	EP-TP.2
EP.86	The signedAttrs of the SignerInfo shall include the pivFASC-N (OID = 2.16.840.1.101.3.6.6) attribute containing the FASC-N of the PIV card.	FIPS 201-1, Section 4.4.2	EP-TP.2
EP.87	The signatureAlgorithm field specified in the SignerInfo field shall be in accordance with Table 3-4 of SP 800-78 and based on the PIV card expiration date in accordance with	SP 800-78, Section 3.2.1	EP-TP.2

	Table 3-3 of SP 800-78.		
EP.88	The SignedData content type shall include the digital signature.	FIPS 201-1, Section 4.4.2	EP-TP.2
EP.89	The digital signature certificate used to sign PIV fingerprint biometric shall in the extKeyUsage assert id-PIV-content-signing (OID = 2.16.840.1.101.3.6.7).	FIPS 201-1, Section 4.4.2	EP-TP.2
EP.90	The size of the public key for digital signature certificate used to sign the biometrics shall be determined by the expiration of the Card in accordance with Table 3-3 of SP 800-78.	SP 800-78, Section 3.2.1	EP-TP.2
EP.91	The CBEFF_SIGNATURE_BLOCK shall be encoded as a Cryptographic Message Syntax external digital signature as defined in RFC 3852.	FIPS 201-1, Section 4.4.2	EP-TP.2
EP.92	The digital signature is implemented as a SignedData Type.	FIPS 201-1, Section 4.4.2	EP-TP.2
EP.93	The value of the version field of the SignedData content type shall be v1 or v3 based on whether the certificates field is omitted or not.	FIPS 201-1, Section 4.4.2	EP-TP.2
EP.94	The digestAlgorithms field of the SignedData content type shall be in accordance with Table 3-3 of SP 800-78.	SP 800-78, Section 3.2.1	EP-TP.2
EP.95	The eContentType of the encapContentInfo shall be id-PIV-biometricObject (OID = 2.16.840.1.101.3.6.2).	FIPS 201-1, Section 4.4.2	EP-TP.2
EP.96	The encapContentInfo of the SignedData content type shall omit the eContent field.	FIPS 201-1, Section 4.4.2	EP-TP.2
EP.97	If the signature on the facial image biometric was generated with a different key as the signature on the CHUID, the certificates field shall	FIPS 201-1, Section 4.4.2	EP-TP.2



	include only a single certificate in the SignerInfo field which can be used to verify the signature; else the certificates field shall be omitted.		
EP.98	The crls field from the SignedData content type shall be omitted.	FIPS 201-1, Section 4.4.2	EP-TP.2
EP.99	The signerInfos in the SignedData content type shall contain only a single SignerInfo type.	FIPS 201-1, Section 4.4.2	EP-TP.2
EP.100	The SignerInfo type shall use the issuerAndSerialNumber choice for the sid and this shall correspond to the issuer and serialNumber fields found in the X.509 certificate for the entity that signed the biometric data.	FIPS 201-1, Section 4.4.2	EP-TP.2
EP.101	The SignerInfo type shall specify a digestAlgorithm in accordance with Table 3-3 of SP 800-78.	SP 800-78, Section 3.2.1	EP-TP.2
EP.102	The signedAttrs of the SignerInfo shall include the MessageDigest (OID = 1.2.840.113549.1.9.4) attribute containing the hash of the concatenated CBEFF_HEADER and the STD_BIOMETRIC_RECORD.	FIPS 201-1, Section 4.4.2	EP-TP.2
EP.103	The signedAttrs of the SignerInfo shall include the pivSigner-DN (OID = 2.16.840.1.101.3.6.5) attribute containing the subject name that appears in the X.509 certificate for the entity that signed the biometric data.	FIPS 201-1, Section 4.4.2	EP-TP.2
EP.104	The signedAttrs of the SignerInfo shall include the pivFASC-N (OID = 2.16.840.1.101.3.6.6) attribute containing the FASC-N of the PIV card.	FIPS 201-1, Section 4.4.2	EP-TP.2
EP.105	The signatureAlgorithm field specified in the SignerInfo field shall be in accordance with Table 3-4 of SP 800-78 and based on the PIV card expiration date in accordance with	SP 800-78, Section 3.2.1	EP-TP.2

	Table 3-3 of SP 800-78.		
EP.106	The SignedData content type shall include the digital signature.	FIPS 201-1, Section 4.4.2	EP-TP.2
EP.107	The digital signature certificate used to sign PIV facial image biometric shall in the extKeyUsage assert id-PIV-content-signing (OID = 2.16.840.1.101.3.6.7).	FIPS 201-1, Section 4.4.2	EP-TP.2
EP.108	The size of the public key for digital signature certificate used to sign the biometrics shall be determined by the expiration of the card in accordance with Table 3-3 of SP 800-78.	SP 800-78, Section 3.2.1	EP-TP.2
EP.109	The message digest produced as a result of a hash function on the contents of a data object buffer shall be identical to that data object's message digest contained in the security object.	Derived	EP-TP.2
EP.110	The security object buffer shall contain an asymmetric digital signature as specified in RFC (3852).	FIPS 201-1, Section 4.4.2	EP-TP.2
EP.111	The digital signature is implemented as a SignedData Type.	FIPS 201-1, Section 4.4.2	EP-TP.2
EP.112	The value of the version field of the SignedData content type shall be v1.	FIPS 201-1, Section 4.4.2	EP-TP.2
EP.113	The digestAlgorithms field of the SignedData content type shall be in accordance with Table 3-7 of SP 800-78.	SP 800-78, Section 3.2.3	EP-TP.2
EP.114	The eContentType of the encapContentInfo shall be id-icao-ldsSecurityObject (OID = 1.3.27.1.1.1).	FIPS 201-1, Section 4.4.2	EP-TP.2
EP.115	The eContent of the encapContentsInfo field shall contain the encoded contents of the ldsSecurity object.	PKI for Machine Readable Travel Documents Offering ICC	EP-TP.2

		Read-Only Access Version - 1.1, Annex C	
EP.116	The certificates field shall be omitted since it is included in the CHUID.	SP 800-73-1-1, Section 1.8.5	EP-TP.2
EP.117	The digestAlgorithm field specified in the SignerInfo field is in accordance with Table 3-7 of SP 800-78.	SP 800-78, Section 3.2.3	EP-TP.2
EP.118	The signatureAlgorithm field specified in the SignerInfo field shall be in accordance with Table 3-4 of SP 800-78 and based on the PIV card expiration date in accordance with Table 3-3 of SP 800-78.	SP 800-78, Section 3.2.1	EP-TP.2
EP.119	The SignedData content type shall include the digital signature.	Derived	EP-TP.2
EP.120	The card issuer's digital signature key used to sign the CHUID shall also be used to sign the security object.	SP 800-73-1-1, Section 1.8.5	EP-TP.2
EP.121	The signature field in the certificate shall specify an algorithm in the AlgorithmIdentifier in accordance with Table 3-4 of SP 800-78 and based on the certificate expiration date in accordance with Table 3-3 of SP 800-78.	SP 800-78, Section 3.2.1	EP-TP.2
EP.122	If Rivest Shamir Adleman (RSA) with Probabilistic Signature Scheme (PSS) padding is used, the parameters field of the AlgorithmIdentifier type shall assert Secure Hash Algorithm (SHA) 256 (OID = 2.16.840.1.101.3.4.2.1). For the other RSA algorithms, the parameters field is populated with NULL. For Elliptic Curve Digital Signature Algorithm (ECDSA), the parameters field is absent.	X.509 Certificate and CRL Profile for the Common Policy, February 6, 2006, Worksheet 9	EP-TP.2
EP.123	The subjectPublicKeyInfo field shall assert an algorithm in the AlgorithmIdentifier in accordance	SP 800-78, Section 3.2.2	EP-TP.2

	with Table 3-5 of SP 800-78.		
EP.124	If the public key algorithm is Elliptic Curve, then the EcpkParameters field uses either the namedCurve field populated with the appropriate OID from Table 3-6 of SP 800-78 or the implicitlyCA choice.	SP 800-78, Section 3.2.2	EP-TP.2
EP.125	The keyUsage extension shall assert only the digitalSignature bit. No other bits shall be asserted.	X.509 Certificate and CRL Profile for the Common Policy, February 6, 2006, Worksheet 9	EP-TP.2
EP.126	The policyIdentifier field in the certificatePolicies must assert id-fpki-common-authentication (OID = 2.16.840.1.101.3.2.1.3.13).	X.509 Certificate and CRL Profile for the Common Policy, February 6, 2006, Worksheet 9	EP-TP.2
EP.127	The authorityInfoAccess field shall contain an id-ad-ocsp accessMethod. The access location uses the Uniform Resource Identifier (URI) name form to specify the location of an Hypertext Transfer Protocol (HTTP) accessible Online Certificate Status Protocol (OCSP) Server distributing status information for this certificate.	X.509 Certificate and CRL Profile for the Common Policy, February 6, 2006, Worksheet 9	EP-TP.2
EP.128	The FASC-N shall be populated in the subjectAltName extension using the pivFASC-N attribute (OID = 2.16.840.1.101.3.6.6).	FIPS 201-1, Section 4.3	EP-TP.2
EP.129	The piv-interim extension (OID = 2.16.840.1.101.3.6.9.1) shall be present and contain an interim_indicator field which is populated with a Boolean value. This extension is not critical.	X.509 Certificate and CRL Profile for the Common Policy, February 6, 2006, Worksheet 9	EP-TP.2
EP.130	The size of the public key for PIV authentication shall be determined by the expiration of the certificate in	SP 800-78, Section 3.1	EP-TP.2

	accordance with Table 3-1 of SP 800-78.		
EP.131	The public key present in the PIV authentication certificate correspond to the PIV authentication private key.	FIPS 201-1, Section 4.3	EP-TP.2
EP.132	The FASC-N in the subjectAltName field in the PIV authentication certificate is the same as the FASC-N present in the CHUID.	Derived	EP-TP.2
EP.133	The expiration of the PIV authentication certificate is not beyond the expiration of the CHUID.	FIPS 201-1, Section 4.3	EP-TP.2
EP.134	If the public key algorithm is RSA, the exponent shall be greater than or equal to 65,537.	SP 800-78, Section 3.1	EP-TP.2
EP.135	The signature field in the certificate shall specify an algorithm in the AlgorithmIdentifier in accordance with Table 3-4 of SP 800-78 and based on the certificate expiration date in accordance with Table 3-3 of SP 800-78.	SP 800-78, Section 3.1	EP-TP.2
EP.136	If RSA with PSS padding is used, the parameters field of the AlgorithmIdentifier type shall assert SHA-256 (OID = 2.16.840.1.101.3.4.2.1). For the other RSA algorithms, the parameters field is populated with NULL. For ECDSA, the parameters field is absent.	X.509 Certificate and CRL Profile for the Common Policy, February 6, 2006, Worksheet 5	EP-TP.2
EP.137	The subjectPublicKeyInfo field shall assert an algorithm in the AlgorithmIdentifier in accordance with Table 3-5 of SP 800-78.	SP 800-78, Section 3.2.2	EP-TP.2
EP.138	If the public key algorithm is Elliptic Curve, then the EcpkParameters field uses either the namedCurve field populated with the appropriate OID from Table 3-6 of SP 800-78 or the implicitlyCA choice.	SP 800-78, Section 3.2.2  X.509 Certificate and CRL Profile for the Common Policy, February	EP-TP.2

		6, 2006, Worksheet 5	
EP.139	The keyUsage extension shall assert both the digitalSignature and nonRepudiation bits. No other bits shall be asserted.	X.509 Certificate and CRL Profile for the Common Policy, February 6, 2006, Worksheet 5	EP-TP.2
EP.140	The size of the public key for digital signature shall be determined by the expiration of the certificate in accordance with Table 3-1 of SP 800-78.	SP 800-78, Section 3.1	EP-TP.2
EP.141	The public key present in the digital signature certificate corresponds to the digital signature private key.	FIPS 201-1, Section 4.3	EP-TP.2
EP.142	The expiration of the digital signature certificate is not beyond the expiration of the CHUID.	SP 800-78, Section 3.1	EP-TP.2
EP.143	If the public key algorithm is RSA, the exponent shall be greater than or equal to 65,537.	SP 800-78, Section 3.1	EP-TP.2
EP.144	The signature field in the certificate shall specify an algorithm in the AlgorithmIdentifier in accordance with Table 3-4 of SP 800-78 and based on the certificate expiration date in accordance with Table 3-3 of SP 800-78.	SP 800-78, Section 3.2.1	EP-TP.2
EP.145	If RSA with PSS padding is used, the parameters field of the AlgorithmIdentifier type shall assert SHA-256 (OID = 2.16.840.1.101.3.4.2.1). For the other RSA algorithms, the parameters field is populated with NULL. For ECDSA, the parameters field is absent.	X.509 Certificate and CRL Profile for the Common Policy, February 6, 2006, Worksheet 5	EP-TP.2
EP.146	The subjectPublicKeyInfo field shall assert an algorithm in the AlgorithmIdentifier in accordance with Table 3-5 of SP 800-78.	SP 800-78, Section 3.2.2	EP-TP.2

EP.147	If the public key algorithm is Elliptic Curve, then the EcpkParameters field uses either the namedCurve field populated with the appropriate OID from Table 3-6 of SP 800-78 or the implicitlyCA choice.	SP 800-78, Section 3.2.2	EP-TP.2
EP.148	If the public key algorithm is RSA, then the keyUsage extension shall only assert the keyEncipherment bit.	X.509 Certificate and CRL Profile for the Common Policy, February 6, 2006, Worksheet 5	EP-TP.2
EP.149	If the public key algorithm is Elliptic Curve, then the keyUsage extension shall only assert the keyAgreement bit.	X.509 Certificate and CRL Profile for the Common Policy, February 6, 2006, Worksheet 5	EP-TP.2
EP.150	The size of the public key for key management shall be determined by the expiration of the certificate in accordance with Table 3-1 of SP 800-78.	SP 800-78, Section 3.1	EP-TP.2
EP.151	The public key present in the key management certificate corresponds to the key management private key.	FIPS 201-1, Section 4.3	EP-TP.2
EP.152	If the public key algorithm is RSA, the exponent shall be greater than or equal to 65,537.	SP 800-78, Section 3.1	EP-TP.2
EP.153	The signature field in the certificate shall specify an algorithm in the AlgorithmIdentifier in accordance with Table 3-4 of SP 800-78 and based on the certificate expiration date in accordance with Table 3-3 of SP 800-78.	SP 800-78, Section 3.2.1	EP-TP.2
EP.154	If RSA with PSS padding is used, the parameters field of the AlgorithmIdentifier type shall assert SHA-256 (OID = 2.16.840.1.101.3.4.2.1). For the other RSA algorithms, the parameters field	X.509 Certificate and CRL Profile for the Common Policy, February 6, 2006, Worksheet 6	EP-TP.2

	is populated with NULL. For ECDSA, the parameters field is absent.		
EP.155	The subjectPublicKeyInfo field shall assert an algorithm in the AlgorithmIdentifier in accordance with Table 3-5 of SP 800-78.	SP 800-76, Section 3.2.2	EP-TP.2
EP.156	If the public key algorithm is Elliptic Curve, then the EcpkParameters field uses either the namedCurve field populated with the appropriate OID from Table 3-6 of SP 800-78 or the implicitlyCA choice.	SP 800-78, Section 3.2.2  X.509 Certificate and CRL Profile for the Common Policy, February 6, 2006, Worksheet 6	EP-TP.2
EP.157	The keyUsage extension shall assert only the digitalSignature bit. No other bits shall be asserted.	X.509 Certificate and CRL Profile for the Common Policy, February 6, 2006, Worksheet 6	EP-TP.2
EP.158	The policyIdentifier field in the certificatePolicies must assert id-fpki-common-cardAuth (OID = 2.16.840.1.101.3.2.1.3.17).	X.509 Certificate and CRL Profile for the Common Policy, February 6, 2006, Worksheet 6	EP-TP.2
EP.159	The extKeyUsage extension shall assert id-PIV-cardAuth (OID = 2.16.840.1.101.3.6.8). This extension is critical.	X.509 Certificate and CRL Profile for the Common Policy, February 6, 2006, Worksheet 6	EP-TP.2
EP.160	The authorityInfoAccess field shall contain an id-ad-ocsp accessMethod. The access location uses the URI name form to specify the location of an HTTP accessible OCSP Server distributing status information for this certificate.	X.509 Certificate and CRL Profile for the Common Policy, February 6, 2006, Worksheet 6	EP-TP.2
EP.161	The FASC-N shall be populated in the subjectAltName extension using the pivFASC-N attribute OID =	X.509 Certificate and CRL Profile for the Common	EP-TP.2



	2.16.840.1.101.3.6.6).	Policy, February 6, 2006, Worksheet 6	
EP.162	The piv-interim extension (OID = 2.16.840.1.101.3.6.9.1) shall be present contain an interim_indicator field which is populated with a Boolean value. This extension is not critical.	X.509 Certificate and CRL Profile for the Common Policy, February 6, 2006, Worksheet 6	EP-TP.2
EP.163	The size of the public key for card authentication shall be determined by the expiration of the certificate in accordance with Table 3-1 of SP 800-78.	SP 800-76, Section 3.1	EP-TP.2
EP.164	The public key present in the card authentication certificate correspond to the card authentication private key.	FIPS 201-1, Section 4.3	EP-TP.2
EP.165	The FASC-N in the subjectAltName field in the card authentication certificate is the same as the FASC-N present in the CHUID.	Derived	EP-TP.2
EP.166	If the public key algorithm is RSA, the exponent shall be greater than or equal to 65,537.	SP 800-78, Section 3.1	EP-TP.2

Table 1 - Applicable Requirements

## 3.2 Test Components

### 3.2.1 Baseline Configuration

The baseline configuration describes initial state of the Test System and its associated components. A Lab Engineer commences execution of this test procedure after performing the necessary updates to the baseline configuration based on the requirements of the test cases described below.

The test system includes the following components as part of its baseline configuration:

1. The Test System – It includes the workstation, the SP 800-85B conformance tool, related software, and the necessary drivers for the CREADER.

### 3.2.2 Components Details

This section lists all the components required by the Lab to execute this test procedure.

#	Component	Component Details	Identifier
1	Test System	The workstation, running the SP 800-85B conformance test tool.	HOST
2	PIV Card Reader (contact)	TBD	CREADER
3	The populated PIV Card which is under test	-	PROD

Table 2 - Test Procedure: Components

### 3.3 Test Cases

This section discusses the various test cases that are needed to test the populated PIV Card against the requirements mentioned above.

#### 3.3.1 Test Case EP-TP.1

##### 3.3.1.1 Purpose

The purpose of this test is to verify whether the PIV Card submitted will allow data to be written to the card without first performing a cryptographic challenge response with the card.

##### 3.3.1.2 Test Setup

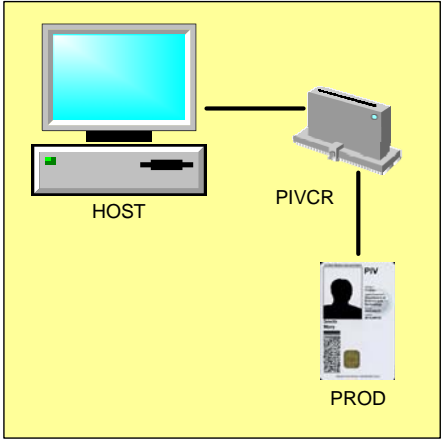
<b>Equipment:</b>	<p>The following components are necessary for executing this test case:</p> <ul style="list-style-type: none"> <li>▪ HOST</li> <li>▪ CREADER</li> <li>▪ PROD</li> </ul>
<b>Configuration Diagram:</b>	 <p>The diagram illustrates the test setup. A yellow rectangular area contains three components: a desktop computer labeled 'HOST' on the left, a PIV Card Reader labeled 'PIVCR' in the center, and a PIV Card labeled 'PROD' at the bottom. A horizontal line connects the HOST to the PIVCR. A vertical line connects the PIVCR to the PROD card. The PIV card shows a silhouette of a person and the text 'PIV' and 'PROD'.</p>

Figure 1 - Configuration Diagram for Test Case EP-TP.1

<b>Preparation:</b>	<ul style="list-style-type: none"> <li>▪ Connect the CREADER into the appropriate port on the HOST.</li> <li>▪ Verify that the CREADER is correctly installed by reviewing its presence in list of hardware using the device manager of the host system.</li> </ul>
---------------------	---

### 3.3.1.3 Test Process

<b>Test Steps:</b>	<ol style="list-style-type: none"> <li>1. Select the Test Case radio button corresponding to EP-TP.1</li> <li>2. Make sure the details of PROD are entered into the Test Application by selecting File → Edit Reference Contact Card Implementation Info menu of the top of the Application window (See Figure 7 - Reference Card Information (Contact)).</li> <li>3. Insert PROD into PIVCR.</li> <li>4. Click on the “Execute Test” button. Follow the steps on the screen.</li> <li>5. Verify that the test has completed by viewing the result on the screen.</li> <li>6. Print a copy of the report for PROD.</li> </ol>
<b>Expected Result(s):</b>	<ol style="list-style-type: none"> <li>1. The test completes successfully showing that: <ul style="list-style-type: none"> <li>▪ The data on the PIV card submitted for testing cannot be updated without first completing a cryptographic challenge response with the card.</li> </ul> </li> </ol>

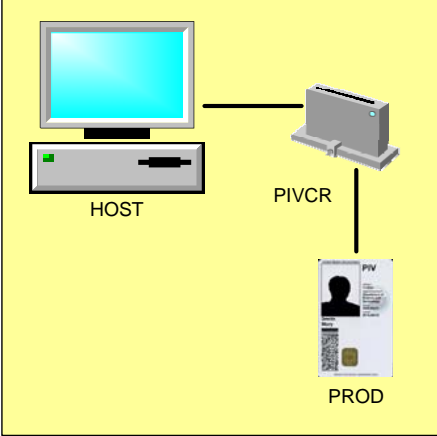
## 3.3.2 Test Case EP-TP.2

### 3.3.2.1 Purpose

The purpose of this test is to verify whether the PIV Card submitted is successfully completing the SP 800-85B data model conformance testing. This conformance testing will ensure all objects loaded on the card, whether mandatory or optional, are formed correctly as defined in FIPS 201 and related publications.

### 3.3.2.2 Test Setup

<b>Equipment:</b>	<p>The following components are necessary for executing this test case:</p> <ul style="list-style-type: none"> <li>▪ HOST</li> <li>▪ CREADER</li> <li>▪ PROD</li> </ul>
-------------------	---

<b>Configuration Diagram:</b>	 <p>The diagram shows a computer system labeled 'HOST' connected to a device labeled 'PIVCR'. The 'PIVCR' is connected to a card labeled 'PROD' (PIV Card). The entire setup is enclosed in a yellow rectangular box.</p> <p><b>Figure 2 - Configuration Diagram for Test Case EP-TP.2</b></p>
<b>Preparation:</b>	<ul style="list-style-type: none"> <li>▪ Connect the CREADER into the appropriate port on the HOST.</li> <li>▪ Verify that the CREADER is correctly installed by reviewing its presence in list of hardware using the device manager of the host system.</li> </ul>

### 3.3.2.3 Test Process

<b>Test Steps:</b>	<ol style="list-style-type: none"> <li>1. Insert the PROD into the CREADER</li> <li>2. Execute the SP 800-85B conformance tool</li> <li>3. <i>&lt;Intermediate steps are unknown at this time&gt;</i></li> <li>4. Verify that the test has completed by viewing the result on the screen.</li> <li>5. Print a copy of the report for PROD.</li> </ol>
<b>Expected Result(s):</b>	<ol style="list-style-type: none"> <li>1. The test completes successfully showing that: <ul style="list-style-type: none"> <li>▪ The objects on the PIV Card are conformant to the requirements of SP 800-85B.</li> </ul> </li> </ol>

## 4 Electronic Personalization Test Application Screens

### 4.1 Testing Screen

The following represents a screen shot of the test application while performing the test for the populated PIV Card.

*<To be provided when screen shot is available>*

### 4.2 Test Report Screen

The following represents a screen shot of the test report that is generated by the Test Application after the Electronic Personalization testing has been completed. It provides the Lab Engineer with a reference of what to expect as a result of successful execution of the test procedure. A Lab Engineer is not expected to fill out any portion of the report manually.

*<To be provided when screen shot is available>*

### 4.3 SP 800-85B Testing Screen

The following screenshot is of the NIST 800-85B Data Conformance Test Tool.

*<To be provided when screen shot is available>*

### 4.4 SP 800-85B Test Report Screen

The following represents a screen shot of the test report that is generated by the NIST 800-85B application after testing the populated PIV Card against the specifications for the different data elements. It provides the Lab Engineer with a reference of what to expect as a result of successful execution of the test procedure.

*<To be provided when screen shot is available>*